

reverse engineering of a
#fraudsters'
#brain

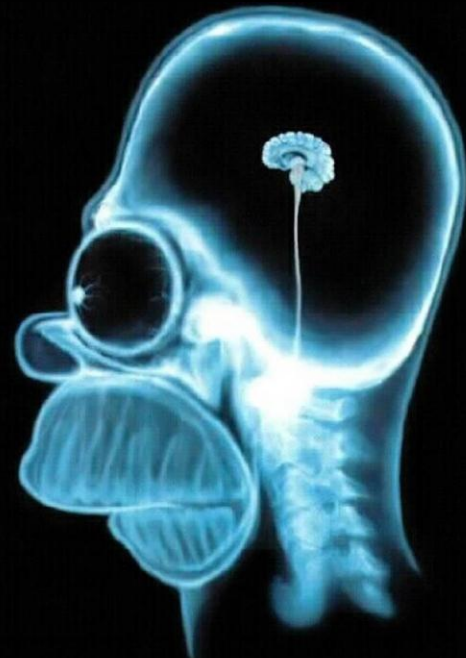
@neyolov evgeny

syscan360 | beijing



#whoami

- cybercrime analysis
- sap hacking and forensics
- erp security analyst @ erpscan
- zeronights hacking conference
- russian defcon group #7812



#about

- project for a gambling company
- anti-fraud black-box testing
- improvement of fraudulent behavior analysis



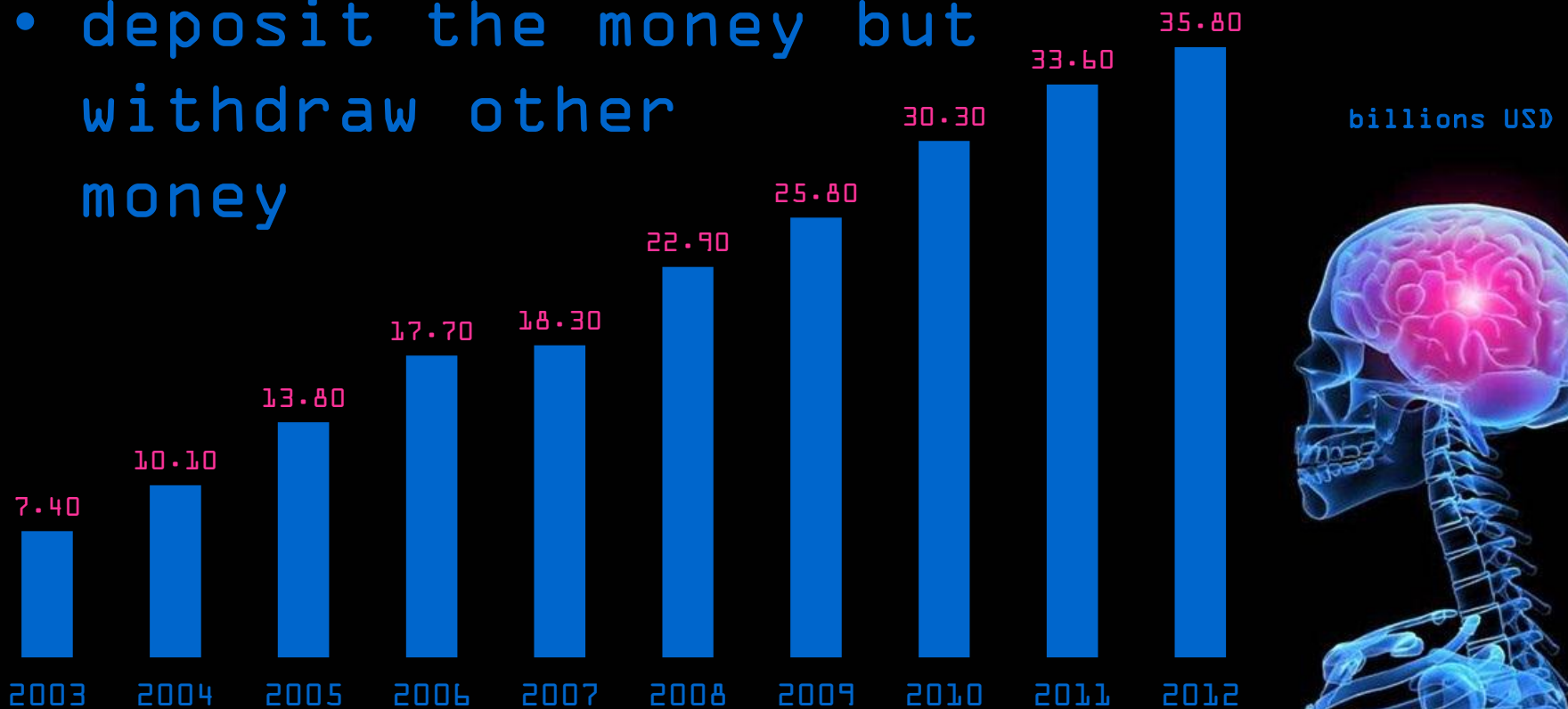
#gambling

- fast growing
- huge market
- no boundaries
- will live forever



#interest

- huge growing market
- uncontrolled money blackhole
- deposit the money but withdraw other money



#problems

- ignoring privacy laws
- ignoring data protection
- demand only scans of personal IDs
- location in offshore areas
- terrorist financing
- money laundering
- carding, etc.



#example

- 15 april 2011 - black friday
- second world largest poker room
- burst like a bubble
- full of fraud - fraudsters + owners
- the most attractive platform for all kinds of fraud



#impunity

- confident of their impunity
- economically inefficient to litigate
- internal investigations only
- max. punishment is a ban
- gambling industry vs. law



#legal cases

- almost unknown

exception:

- man jailed for bonus abuse
- £80,000 ~ \$130,000
- fraudulent international
passports, identity cards,
false utility bills



#scope

major:

- poker
- casino
- betting

minor:

- bingo
- lottery
- etc.



#confrontation

- player control
- anti-fraud checks

vs.

- stuff
- c2c-market
- fraud coaching
- community wisdom



#kyc

- identity
- location
- financial information
- place and date of birth
- e-mail and telephone number
- personal residence address



#kyc

- identity
 - stolen/fake passports
- location
 - IP addresses, fake bills
- financial information
 - fake bills
- place and date of birth
 - stolen/fake passports
- e-mail and telephone number
 - underground call services
- personal residence address
 - fake apartment accounts



#checks

- operating system IDs
- browser user agent
- system registry
- hardware IDs
- MAC address
- IP address



#checks

- operating system IDs
 - ID randomization software
- browser user agent
 - user agent switchers
- system registry
 - registry cleaners
- hardware IDs
 - ID randomization software
- MAC address
 - MAC changers
- IP address
 - VPN, socks



#checks

- operating system IDs
 - ID randomization software
- browser user agent
 - user agent switchers
- system registry
 - registry cleaners
- hardware IDs
 - ID randomization software
- MAC address
 - MAC changers
- IP address
 - VPN, socks
- one episode = one host



#stuff

virtual machines:

- ID randomization software
- anti-detect patches



#stuff

dedicated servers:

- bruteforced hosts
- unique environment
- enterprise/datacenter/private server or client system
- one-off usage



#activity

- credit card fraud
- account takeover
- bonus hunting
- abuse affiliate programs
- unfair play



#carding

- identity theft
- stolen credit card data
- stolen cardholder information
- 2 scenarios



#carding scenario 1

full kit for bypassing checks:

- credit card data
- hardcopy/photocopy of personal ID
- system environment according to the above info



FULLZ CC:	Fullz info:	Address 1:	Name On Card:
	Address 2:		Credit Card Number:
Name and surname:	City:		Credit Card Brand:
billing adress:	State:		Credit Card Type:
Address 1:	Zip:		Start Date:
Address 2:	Country:		EXP Date:
City:	Home Phone:		issue Number:
State:	Date Of Birth:		Credit Card PIN Number:
Zip:	Social Security Number:		Card ID Number:
Country:	Mothers Maiden Name:		Card Bank Name:
Home Phone:	Drivers License Number:		Card 1800 Number:
Name On Card:	Drivers License State:		email:
Credit Card Number:	Secret Question 1:		email pass:
Credit Card Type:	Secret Question Answer 1:		bank name:
EXP Date:	Secret Question 2:		Bank Account Number :
email:	Secret Question Answer2:		Bank Routing Number :
			bank phone:

#carding scenario 2

game "lucky fraudster":

- PAN
- photoshopped/generated/fake IDs
- social engineering skills



#carding scenario 2

- i need PAN and cardholder name.
- is it all? are you kidding me?
- ismycreditcardstolen.com
- twitter.com/needadebitcard



Debit Card

@NeedADebitCard

Please quit posting pictures of you



Niko S @nicknikoo

Debit card Chelsea Stamford Bridge pic.twitter.com/njkjD3QK

Retweeted by Debit Card

Hide photo Reply Retweet Favorite

26 Nov



3
RETWEETS

1
FAVORITE



6:41 AM - 26 Nov 12 - Details

Flag media

Reply to @nicknikoo



Major Hayden @rackerhacker

@nicknikoo Thanks for sharing. Can I buy something on your card?

Expand

26 Nov

Twe



Tweet to Debit Card

@NeedADebitCard

Tweets

Following

Followers

Favorites

Lists

Recent images



Similar to Debit Card



Gerd Eist @erdgeist

Follow

#account takeover

- who is to blame?
- the gambling operator
- weak password recovery validation
- server-side vulnerabilities
- client-side vulnerabilities
- data breaches



#account takeover

- who is to blame?
- the player
- sensitive personal information disclosure
- victim of malware, spyware, phishing



#account takeover

- stealing all funds off an account
- obtaining ownership in case account identity was not confirmed yet
- using account balance as a transit point for fraudulent money
- selling access to the account on underground market
- spending money for fun



#bonus hunting

- violation of Terms of service
- no hacked player accounts
- no victims among players
- no stolen player funds



#bonus hunting

- affiliate programs abuse
- bonus offers abuse
- arbitrage betting
- other unfair activities like chip dumping, cheating, using bots to wager, etc.



#affiliate program abuse

- register affiliate account
- register fake player
- ????
- PROFIT!!!!



#affiliate program abuse

- gambling operators have programs for attracting new players
- programs provided by professional marketing companies
- companies always looking for affiliate partners
- fraudsters always looking for money



#bonus offer abuse

- welcome
- reload
- no deposit
- moneyback
- sticky



#arbitrage betting

- two accounts
- two outcomes
- two bets
- one win
- guaranteed win
for the player
- guaranteed loss
for the operator



#ctf

- capture the fraudster
- different schemes, but parts of internal processes are similar
- often involve one account into several fraud episodes



#ctf

- c2c underground market
- random account from the list of bruteforced dedicated servers
- is there anything sacred for dealer in stolen goods?
- 1 account - 1 customer.
Oh, really?





#case 1

- security event log, logon/logoff
- event ID 4624 (7) or 528 (XP)
- logon type 10 (via RDP)
- server username
- domain name
- logon type
- client hostname
- IP address





- События страницы сводки
- Журналы Windows
 - Приложение
 - Безопасность
 - Установка
 - Система
 - Перенаправленные события
- Журналы приложений и служб
 - Internet Explorer
 - Key Management Service
 - Media Center
 - Microsoft
 - Windows
 - API-Tracing
 - AppID
 - Application-Experience
 - AppLocker
 - Audio
 - Authentication User Interf...
 - Backup
 - Biometrics
 - Bits-Client
 - Bluetooth-MTPEnum
 - BranchCache
 - BranchCacheSMB
 - CAPI2
 - CertificateServicesClient-C
 - CertPolEng
 - CodeIntegrity
 - CorruptedFileRecovery-Cli
 - CorruptedFileRecovery-Se
 - DateTimeControlPanel

Свойства событий - Событие 4624, Microsoft Windows security auditing.

Общие Подробности

☒ Понятное представление ☐ Режим XML

TargetUserSid S-1-5-21-38503254-1057719598-1857940269-1000

TargetUserName [REDACTED]

TargetDomainName [REDACTED]

TargetLogonId 0x95cc43e

LogonType 10

LogonProcessName User32

AuthenticationPackageName Negotiate

WorkstationName [REDACTED]

LogonGuid {00000000-0000-0000-0000-000000000000}

TransmittedServices -

LmPackageName -

KeyLength 0

ProcessId 0x17f8

ProcessName C:\Windows\System32\cmd.exe

IpAddress [REDACTED]

IpPort 1192

Копировать

Код события
4672
4624
4624
4648
4624
4672
4672
4634
4634
4624
4624
4634

WWW.IP-SCORE.COM

if we see, then others see..

Enter IP for check

Check

IP information:

[REDACTED]	Russian Federation
State:	Moscow City
City:	Moscow
ZIP:	N/A
Hostname:	[REDACTED] Whois
Organization:	VL-Telecom Ltd
ISP:	VL-Telecom Ltd

- IP address

#case 1

applications and services logs -
microsoft - windows tree

TerminalServices-*:

- RDPClient
- PnPDevices
- ClientUSBDevices
- LocalSessionManager
- RemoteConnectionManager



#case 2

- start menu? are you kidding me?

- fraud target
- hardware ID randomizer
- instant messenger



Cavalliere 

 27.01.2012, 02:45

nikobellic

jid: nikobellic@exploit.im

icq: 174314 и 174-314

И так ситуация конечно трудная но она есть

► Продажа покер акков

nikobellic 

 5.10.2009, 21:48

WANTED
ESSENT WITH A DEADLY WEAPON



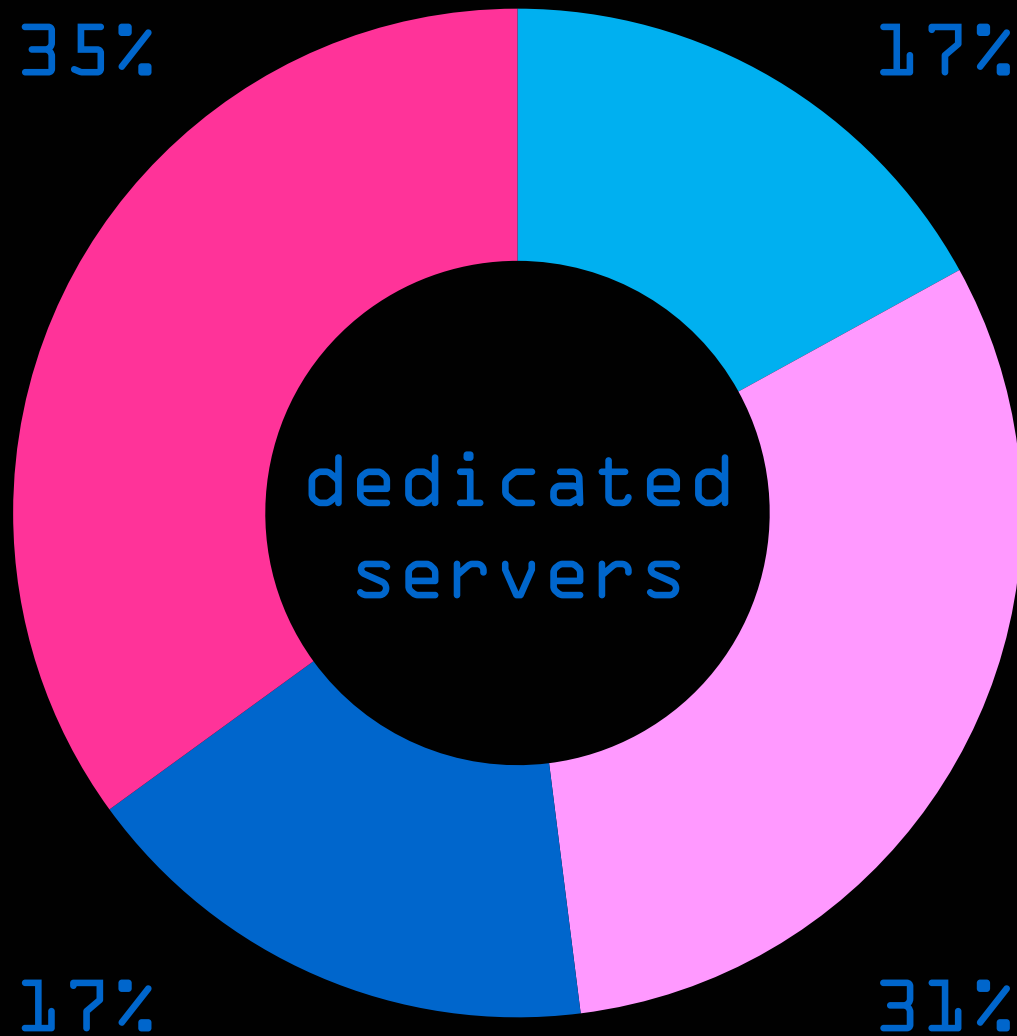
Продаю акки покера ,фултилт балансы от 500
цена за 500\$- 40wmz, + дедик в комплекте



DOUBLE FACEPALM

When the Fail is so strong, one Facepalm is not enough.

#evidence



#the grugq's wisdom

it seems his favorite phrase

no logs - no crime

dear fraudsters
please
make our work
a little harder
and more interesting



#suggested reading

- global gaming outlook <http://goo.gl/PntLS>
- a gamble or a sure bet? <http://goo.gl/n8YYZ>
- gambling knowledgebase <http://goo.gl/wmvsc>
- jailed for bonus abuse <http://goo.gl/vttJ7>
- AML and CTF <http://goo.gl/lWqUi>



#you are welcome ^_^

twitter.com/neyolov
neyolov@erpscan.com

